It is a long way to … e-evidence: EU reforms in the collection of electronic evidence Part 2: The role of service providers

On 25 January 2023, the Council of the EU confirmed an agreement with the European Parliament has been reached on both the draft regulation and the draft directive on cross-border access to e-evidence. The first part of this article focused on the description of the instrument, as proposed by the Commission back in 2018, by explaining how it departs from traditional mutual recognition instruments and mutual legal assistance (MLA) agreements and highlighted some of the concerns raised by relevant stakeholders. This second part will discuss the role of service providers. It will present the approach put forth by the EU institutions to assess the degree to which service providers are involved, and reflect on some choices made by the EU institutions in the final compromise.

Origin of the re-allocation of protective functions in the Commission's proposal: service providers as 'addressees' of orders

As highlighted in the first part of this article and by other scholars (see here, here, and here), the e-evidence Regulation introduces a new form of cross-border cooperation, which has raised several significant legal questions, the role of service providers being one of them. The approach chosen by the Commission regarding service providers has been described by some critics as a re-allocation of protective functions. This is due to the fact that under the Commission's proposed Regulation, the legal representative of the service provider is given the role of the 'addressee' of European Production Order (EPO) and European Preservation Order (EPsO). In practice, a competent judicial authority in the EU, the issuing authority, will address an order – to preserve or to produce data – through a standardised certificate directly to the service provider's legal representative in the EU and the data will be provided directly to the issuing authority.

Under the Commission's approach the state where the order is executed is only assigned a very limited role of review at the enforcing stage which means that this state may only have a say if the service provider refuses to comply with the order. *A contrario*, when the service provider complies with an order, the enforcing state might not even be aware of the existence of the order, neither will it be able to object. Therefore, the enforcing state will not be able to exercise its protective functions by refusing to execute orders on fundamental rights' grounds, as traditionally allowed by mutual recognition instruments (see for instance, Art. 11(1)(f) of the European Investigation Order Directive). The protective functions are assigned to the competent authority in the issuing state and, to some extent, to the addressee of the order, a private actor.

No intended role to no role at all?

Despite the criticism voiced by civil society, service providers and the European Parliament that the proposal re-allocated protective functions to service providers, the Commission shaped their role in a way that allows us to question whether it did indeed intend for private actors to exercise such functions. The Commission's proposed Regulation contained several grounds for service providers to refuse to execute orders as well as grounds to oppose their enforcement. The most significant one being outlined in Article 9(5), subparagraph 2 of the proposed Regulation. It states that the addressee, i.e., the service provider's legal representative, may refuse to execute an EPO if it is apparent that it 'manifestly violates the [EU Charter of

Fundamental Rights]' or that it is 'manifestly abusive'. If the service provider does not comply with its obligation, the Member State where it is addressed steps in to enforce the order. At this stage, the service provider may oppose the EPO based on the same grounds (see Arts 14(4)(f) and 14(5)(e)).

Therefore, it is submitted that the protective functions delegated to service providers can only be described as limited, if not weak. This fundamental rights clause is limited to 'manifest' violations that are 'apparent from the sole information contained in the order'. However, in practice, the service provider will not receive the full order, only a certificate which will contain less information than contained in the order. The limited information contained in the certificate will make it extremely challenging (if not entirely impossible) for service providers to undertake any sort of fundamental rights assessment. Under the European Commission's proposal, the issuing Member State is required to provide the grounds for the necessity and proportionality of the measure (Arts 6(3)(g) and 5(5)(i)). Although this condition is required for issuing orders, it will not be included in the certificate sent to the service provider's legal representative. In fact, the proposed Regulation excludes this information from the list of information that must be contained in the certificate.

The term 'manifest' has not been defined but one can argue that such a clause may be interpreted as preventing service providers from undertaking a fundamental rights assessment. The Commission itself recognises, in the Explanatory Memorandum to its proposal, that the ground allowing service providers to refuse to execute an order because it 'manifestly violates the Charter' or is 'manifestly abusive' will be applicable only in exceptional cases. Orders seeking the production of content data relating to undefined groups of people in a geographical area or with no link to concrete criminal proceedings were cited as examples by the Commission.

In the Council General Approach, Member States took a more drastic step by deleting the fundamental rights clause from the grounds upon which service providers are permitted to refuse to execute orders in its entirety. Leaving the issuing authority as the sole assessor of fundamental rights considerations. As argued here, by deleting the fundamental rights clause, the Council might have wanted to limit the role of the service provider as the guardian of fundamental rights, which the Commission's version might have intended to entrust in them.

The European Parliament re-introduced the intervention of a second Member State (i.e. the executing state) which has altered the way direct cooperation functions and shifted responsibilities back to Member State authorities. The option chosen by the Parliament was for orders to be addressed to the service provider and to the executing authority simultaneously (see Art. 7(1) of the Report). An additional feature added was that of a double notification mechanism, with or without suspensive effect, depending on the data category sought by the order. This issue, discussed further here, generated tensions between Member States who strongly diverged on the extent, content, and outcome of such a system. Despite its strong opposition to the role of service providers, the Report still maintained some space for service providers to flag issues by allowing those actors to inform the executing authority that an order is manifestly abusive or exceeds the purpose of the order (see Arts 8a(7), 9(5)(2) and 10(6)).

What is left to service providers: the compromise text

Ultimately, the EU institutions have upheld the approach put forward by the European Parliament and maintained (to some extent) the involvement of a second Member State and opted for a far more limited role for service providers. The compromise text implements a

notification mechanism to the enforcing Member State. This mechanism is however limited to EPOs for traffic data and content data (see Art. 7a) and encompasses a suspensive effect. It prevents the service provider to transmit data to the issuing authority until the enforcing authority decides, within 10 days of receipt of the order, whether to raise a ground for refusal (see Art. 9 compromise text). *A contrario*, there is no need for notification when it comes to EPOs issued to produce subscriber data and data requested for the sole purpose of identifying the user, nor is notification required for EPSOs. The scope of the enforcing authority's protective functions has therefore been narrowed down to the most intrusive orders.

Furthermore, the fundamental rights clause contained in Article 10(1)(b) is worded in such strict terms that it may prove difficult for the executing authority to refuse the execution of an order. The clause is meant to be used only in 'exceptional situations' and sets a high threshold for its application. The executing authority is required to provide specific and objective evidence showing that there are substantial grounds to believe that the order entails 'a manifest breach' of a relevant fundamental right. Here again, the use of the word 'manifest' is unfortunate and does not find precedent in previous mutual recognition instruments. The origin of this ground seems to stem from the case-law of the Court of Justice of the EU (CJEU) in relation to the European Arrest Warrant, especially Aranyosi and Căldăraru.

With regard to service providers, the compromise text does not grant them the possibility to oppose the execution of a production order but only to flag some specific issues related to the order. Service providers may not be able to comply because of a de facto impossibility (Art. 9(4)). Recital 41a states that it should be assumed if the person whose data is sought is not a customer of the service provider or cannot be identified as such even after a request for further information to the issuing authority, or if the data have been lawfully deleted before receiving the order. In case an EPO is incomplete, contains manifest errors or does not contain sufficient information for the service provider to execute it, communication between the issuing authority and the service provider should take place in order to resolve the issue (Art. 9(3)). Article 9 (2a) gives service providers the possibility to flag interferences with immunities and privileges and rules on the determination or limitation of criminal liability that relate to the freedom of press or the freedom of expression in other media in the enforcing state.

This task may prove rather challenging given that it will have to be based solely on the information contained in the certificate which will contain very little information (see Art. 8(2)). Service providers may also justify not providing the data, not providing it exhaustively, or not providing it within the deadline for other reasons (Art. 9(5)). At first blush, it could be argued that such a ground would offer service providers some sort of leeway when assessing orders. Closer examination of Annex III of the Regulation, however, which lists the reasons for non-execution, refutes that argument. Fundamental rights are only mentioned in the context of conflicting obligations arising from a third country law, with the purpose of identifying the interest protected by the law of the third country (such as the UK).

A final and highly significant consideration is the fact that, unlike national authorities, service providers may be subject to financial sanctions in case of non-compliance. In this regard, the compromise text requires that Member States implement pecuniary sanctions that are effective, proportionate, and dissuasive and sets a rather high minimum standard, 2% of the total worldwide annual turnover of the service provider's preceding financial year (Art. 13). In fact, when the Council, in its General Approach, opted to impose the exact same pecuniary sanction, several stakeholders (see EDPS Opinion 7/2019 and EDRi Recommendations) argued that it may deter service providers from objecting to orders. Furthermore, the compromise text

specifies that such sanctions are without prejudice to national laws providing for the imposition of criminal sanctions. Service providers which fail to comply with orders may therefore face significant consequences, by being subject to financial penalties and even criminal charges, making the stakes rather high for those actors.

Conclusion: some reflections on the EU legislator's choices

In order to prevent the so-called 'privatisation' of public functions or 're-allocation of protective functions', the EU institutions have re-introduced another Member State in the cooperation process and limited the role of service providers. The instrument created by the compromise text does look different from the one initially proposed by the Commission and deserves some further consideration. As explained in Part 1 of this article, the lack of participation of another Member State on the receiving end of an order was perceived as reducing the level of fundamental rights protection. This is because the additional layer of control and scrutiny provided by the said state is removed. While this approach fits the approach followed by classic mutual recognition instrument, it may not be entirely correct to assume that involving the executing Member State offers stronger safeguards for fundamental rights.

The argument here is that the involvement of the executing state is very much rooted into the principle of sovereignty rather than into the creation of further guarantees for the EU citizens, as extensively argued here, and the safeguards for states do not correspond to the definition of safeguards for individuals (i.e. provisions aimed at ensuring that interferences with fundamental rights caused by an investigative measure are proportionate). This argument carries considerable weight when one considers the grounds in the compromise text for refusal which are based, *inter alia*, on considerations linked to immunities and privileges, and the double criminality principle.

This leads us to question whether the executing Member State is the most appropriate and suitable one to review an order. In the digital world, the state where the order is executed is rarely the state where the person concerned by the order resides. This implies that there may not be a match between the territory of the executing Member State and the territory where the person targeted by the order resides. In fact, the designation of the enforcing state will be dictated by the choice of the service provider which will have to designate a Member State as its state of establishment or as the state where its legal representative is located. As Christakis observes, notification to the affected state (instead of the Member State where the person(s) targeted by the order resides) would have had the benefit of focusing on the targeted individual and allowing that state to exercise its protective functions and safeguard the fundamental rights of individuals present in their territory, as required by the European human rights framework.

Finally, this author urged the EU institutions to consider whether service providers may play a part in the protection of fundamental rights and, if so, how, and to what extent. Unfortunately, the e-evidence Regulation is a missed opportunity to address the role of the private sector. As argued here, private actors are already setting up rules, enforcing them, and becoming arbiters between conflicting rights. Such a trend can be observed in the area of content moderation and in the field discussed here, namely the gathering of digital evidence. As emphasized here, addressing the role of service providers is part of a more fundamental question which revolves around the execution of public power and private actors' role in protecting fundamental rights. The current legal framework, including the General Data Protection Regulation, does not reflect nor regulate these new power dynamics (see here for considerations on the concept of 'data power'). In addition, the failure to address the existing role of service providers results in a

failure to reflect on the appropriate means to regulate the private sector. This extends to the rationale and degree to which they should be 'duty-bearers' when it comes to fundamental rights and (as others have highlighted) what would be the added-value of such duties from a citizen's perspective.

Marine Corhay is a PhD candidate at the University of Liège (FRESH grantee, F.R.S.-FNRS) and a Visiting Scholar at the Information Law & Policy Centre (IALS). *Her research stay is funded by the University of Liège (MoDUS grant) and the David-Constant Grant for scientific research stays abroad (Law School, ULiège).*